David S. Casey, Jr., SBN 060768
dcasey@cglaw.com
Gayle M. Blatt, SBN 122048
gmb@cglaw.com
Wendy M. Behan, SBN 199214
wbehan@cglaw.com
CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, CA 92101
Tel: (619) 238-1811; Fax: (619) 544-9232

Deval R. Zaveri, SBN 213501
dev@zaveritabb.com
James A. Tabb, SBN 208188
jimmy@zaveritabb.com
ZAVERI TABB, APC
402 W. Broadway, Ste. 1950
San Diego, CA 92101
Tel: (619) 831-6988; Fax: (619) 239-7800

Attorneys for Plaintiffs and the class

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

Jennifer J. Myers, Paul Dugas, Danielle Beck, Leah Cassell, Pooja Garg, Rajesh Garg, Ashish Gupta, Jessica Jagir, Daniel Margo, Ann Marie Osborne, Susan Park, and **Amar Patel**, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

Yahoo! Inc., a Delaware corporation,

Defendant.

CASE NO. 16-cv-02391-CAB-WVG

First Amended Class Action Complaint for Damages and Equitable Relief

Jury Trial Demanded

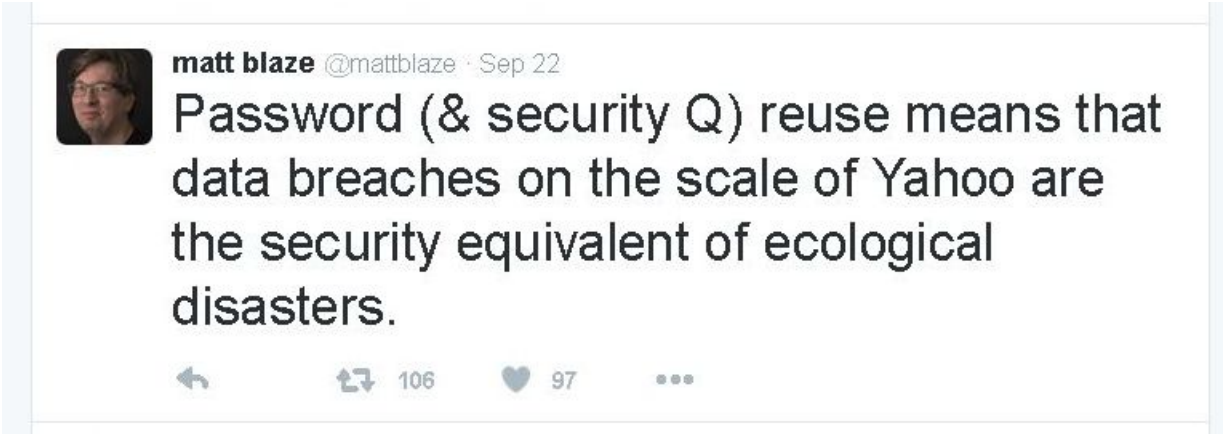
COME NOW Plaintiffs Jennifer J. Myers, Paul Dugas, Danielle Beck, Leah Cassell, Pooja Garg, Rajesh Garg, Ashish Gupta, Jessica Jagir, Daniel Margo, Ann Marie Osborne, Susan Park, and Amar Patel ("Plaintiffs"), on behalf of themselves and all others similarly situated, and for causes of action against the Defendant, complain and allege as follows:

General Allegations

1. This action is brought to seek redress for damages sustained by Plaintiffs and other members of the class as a result of the failure of Defendant Yahoo! Inc. ("Yahoo" or "Defendant") to securely store and maintain the personal information of Plaintiffs and the class.

2. On September 22, 2016, Yahoo announced that account information from roughly 500 million Yahoo user accounts was stolen by online hackers approximately two years ago. This includes names, email addresses, telephone numbers, birth dates, passwords, and security questions (referred to as "Personal Information" or "PI") of Yahoo account holders. This is believed to be the largest data breach in history.

3. Matt Blaze, a cyber security expert and director of the Distributed Systems Lab at the University of Pennsylvania likened the breach to an "ecological disaster."



4. Jurisdiction is proper in this case under 28 U.S.C. § 1332(d) in that the matter in controversy exceeds $5,000,000, there are more than 100 class members, and members of the class are citizens of states different than Yahoo. In addition, Plaintiffs bring a claim under the Federal Stored Communications Act, 18 U.S.C. § 2702, which provides for jurisdiction under 28 U.S.C. § 1331. Venue is proper under 28 U.S.C. § 1391(c) because Yahoo is a corporation that does business in and is subject to personal jurisdiction in this district.

PARTIES

5. Plaintiff Danielle Beck is an individual who resides in San Diego, California. Plaintiff was a Yahoo account holder during the time of the data breach and stored her PI with Yahoo. She suffered actual damages from the data breach. Ms. Beck stores her American Express credit card information with Yahoo and Yahoo automatically charges it to pay for premium Yahoo service. Ms. Beck has needed to get several new cards in the last two years because of repeated fraudulent charges.

6. Plaintiff Leah Cassell is an individual who resides in Evans, Georgia. Plaintiff was a Yahoo account holder during the time of the data breach and stored her PI with Yahoo. She suffered actual damages from the data breach. Ms. Cassell had her debit card information stolen, and had fraudulent withdrawals made from her bank account in May 2016, which she believes is related to the Yahoo breach because, at one point, her bank account username and password were the same as her Yahoo email account username and password. Plaintiff Paul Dugas is an individual who resides in San Diego, California. Plaintiff was a Yahoo account holder during the time of the data breach and stored his PI with Yahoo. Mr. Dugas suffered actual damages from the data breach. At times, Mr. Dugas used the same password across several accounts, including his Yahoo email account. In spring 2016, Mr. Dugas was informed that his identity had been compromised and that a fake federal income tax return had been filed in his name.

7. Plaintiff Pooja Garg is an individual who resides in Philadelphia, Pennsylvania. Plaintiff was a Yahoo account holder during the time of the data breach and stored her PI with Yahoo. She suffered actual damages from the data breach. Ms. Garg's email account has been hacked into several times and spam emails have been sent from her account.

8. Plaintiff Rajesh Garg is an individual who resides in Naperville, Illinois. Plaintiff was a Yahoo account holder during the time of the data breach and stored his PI with Yahoo. He suffered actual damages from the data breach. Mr. Garg used Yahoo email, Flickr, and Yahoo Finance at the time of the breach. Mr. Garg stored personal photo albums on Flickr, and stored his trading and retirement account data with Yahoo Finance. Mr. Garg has had his Yahoo account hacked several times between 2014 and 2016 and has had several embarrassing spam and phishing emails sent from his account to about 500 of his personal and professional contacts.

9. Plaintiff Ashish Gupta is an individual who resides in Bolingbrook, Illinois. Plaintiff was a Yahoo account holder during the time of the data breach and stored his PI with Yahoo. He suffered actual damages from the data breach. Mr. Gupta stores his American Express credit card information with Yahoo and Yahoo automatically charges it to pay for premium Yahoo service.

10. Plaintiff Jessica Jagir is an individual who resides in San Diego, California. Plaintiff was a Yahoo account holder during the time of the data breach and stored her PI with Yahoo. She suffered actual damages from the data breach as alleged below. In particular, in 2014, Ms. Jagir suffered multiple fraudulent transfers from her Schwab account to Budapest near the same time as the Yahoo breach. She did not find out about the transfers until later because the hackers deleted the transfer initiation and receipt emails from her Yahoo inbox and trash. She still gets bogus phishing emails in her Yahoo account.

11. Plaintiff Daniel Margo is an individual who resides in Pharr, Texas. Plaintiff was a Yahoo account holder during the time of the data breach and stored his

PI with Yahoo. He suffered actual damages from the data breach. Mr. Margo's Capital One bank account was linked to his Yahoo account. Since the breach, Mr. Margo has had at least one fraudulent charge made to his Capital One debit card. He also has received notifications from credit agencies about suspicious activity involving his credit.

12. Plaintiff Jennifer J. Myers is an individual who resides in San Diego, California. Plaintiff was a Yahoo account holder during the time of the data breach and stored her PI with Yahoo. She suffered actual damages from the data breach. Ms. Myers used the same username and passwords for her Yahoo email and credit card accounts.

13. Plaintiff Ann Marie Osborne is an individual who resides in San Diego, California. Plaintiff was a Yahoo account holder during the time of the data breach and stored her PI with Yahoo. She suffered actual damages from the data breach. Ms. Osborne believes that her Yahoo account and identity have been breached and hacked because her Yahoo email account password is ineffective, and because when she answered Yahoo's security questions in an attempt to regain access to her account, the answers, all personal information known to her, were rejected as incorrect. Consequently, Ms. Osborne has been locked out of her Yahoo account, and her only personal email account, for weeks.

14. Plaintiff Susan Park is an individual who resides in San Diego, California. Plaintiff was a Yahoo account holder during the time of the data breach and stored her PI with Yahoo. She suffered actual damages from the data breach. Ms. Park has had her yahoo email account hacked into and has had spam sent from her email account. Separately, Ms. Park's bank account is linked to her Yahoo email account. She used the same username for her Yahoo email and bank account, and at times has used the same password for both accounts. Ms. Park has had fraudulent withdrawals made from her bank account as recently as September 2016.

15. Plaintiff Amar Patel is an individual who resides in Johns Creek, Georgia. Plaintiff was a Yahoo account holder during the time of the data breach and stored his PI with Yahoo. Mr. Patel uses his Yahoo account to participate in Yahoo Fantasy Sports Leagues. He suffered actual damages from the data breach.

16. Defendant Yahoo! Inc. is a Delaware corporation registered with the California Secretary of State and is headquartered in Sunnyvale, California.

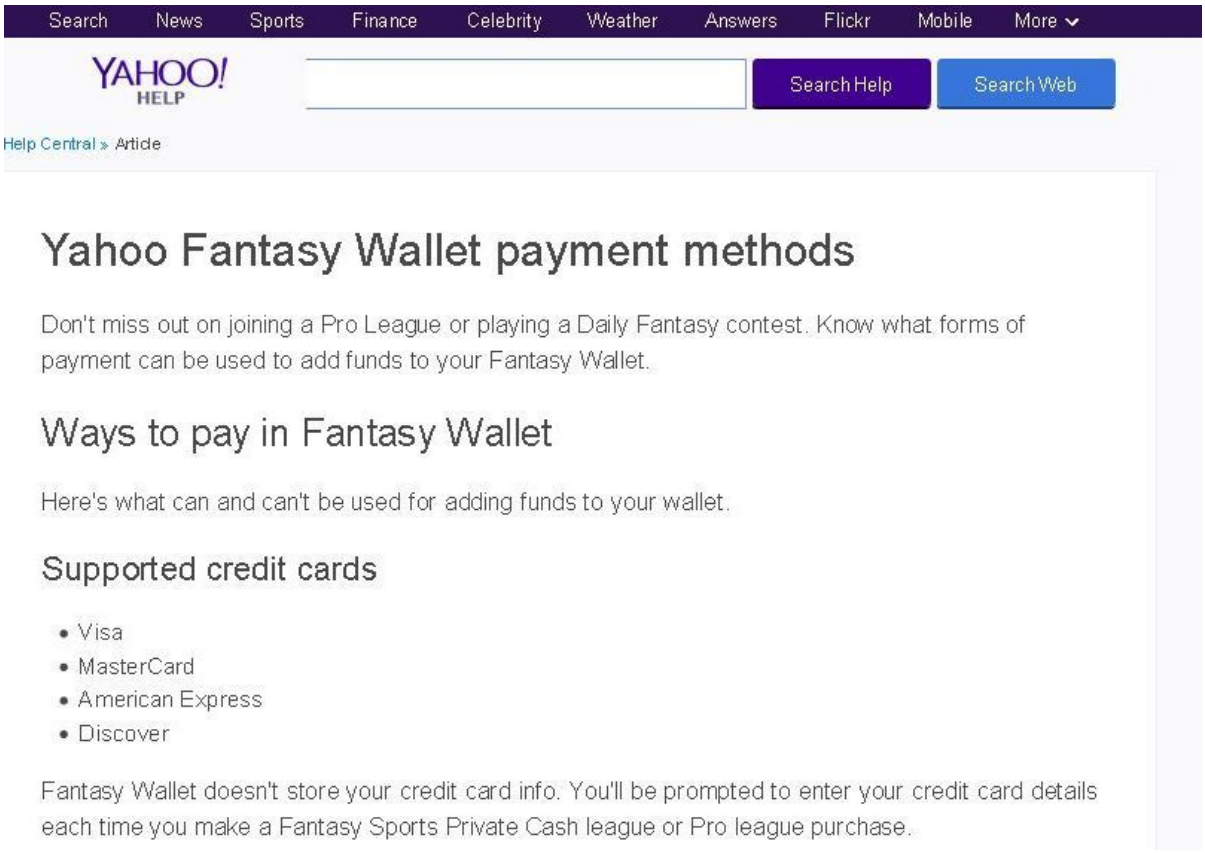
FACTUAL ALLEGATIONS

17. Yahoo was founded in 1994 as a directory of websites, but developed into a source for searches, email, shopping, and news. Currently, its services attract approximately one billion visitors per month. Yahoo sister sites include, among others, Flickr, Yahoo Finance, and Yahoo Fantasy Sports.

18. Yahoo Mail is one of the oldest free email services, and many users have built their digital identities around it, from their bank and stock trading accounts to photo albums and even medical information. Moreover, not only are email addresses used for private communications, but they serve as recovery and log-in credentialing points for accounts on many other websites. Yahoo allows anyone who is over the age of 12 to open a Yahoo account.

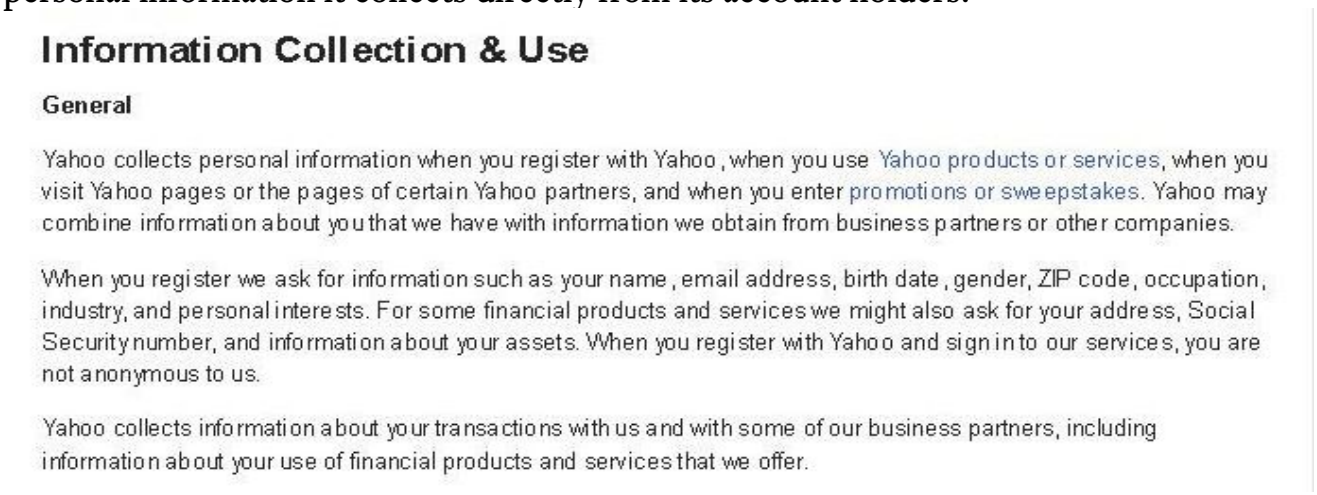
19. Yahoo is central to many other online services, including ones that require entry of credit card and other financial information, such as the popular Yahoo fantasy sports leagues.

20. The Yahoo Fantasy Sports leagues use what Yahoo calls "Yahoo Wallet," in which users can enter a variety of credit card, debit card, and other account information. <*https://help.yahoo.com/kb/SLN26520.html*>



21. Plaintiffs and class members signed up for online Yahoo accounts that required them to provide many different sorts of personal information, including, in some cases, debit and credit card information.

22. The "Privacy Center" portion of Yahoo's website explains the type of personal information it collects directly from its account holders:



<https://policies.yahoo.com/us/en/yahoo/privacy/index.htm>

23. Yahoo also informs its account holders that it does not share personal information:

Information Sharing & Disclosure

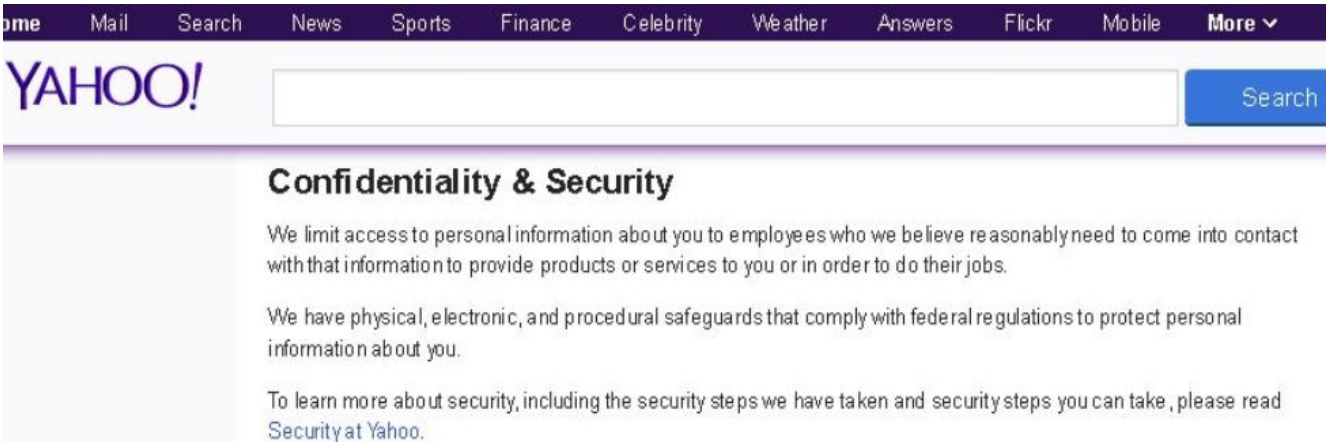
Yahoo does not rent, sell, or share personal information about you with other people or non-affiliated companies except to provide products or services you've requested, when we have your permission, or under the following circumstances:

- We provide the information to trusted partners who work on behalf of or with Yahoo under confidentiality agreements. These companies may use your personal information to help Yahoo communicate with you about offers from Yahoo and our marketing partners. However, these companies do not have any independent right to share this information.
- We have a parent's permission to share the information if the user is a child under age 13. See Children's Privacy & Family Accounts for more information about our privacy practices for children under 13.
- We respond to subpoenas, court orders, or legal process (such as law enforcement requests), or to establish or exercise our legal rights or defend against legal claims.
- We believe it is necessary to share information in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of Yahoo's terms of use, or as otherwise required by law.
- We transfer information about you if Yahoo is acquired by or merged with another company. In this event, Yahoo will notify you before information about you is transferred and becomes subject to a different privacy policy.

Yahoo displays targeted advertisements based on personal information. Advertisers (including ad serving companies) may assume that people who interact with, view, or click targeted ads meet the targeting criteria—for example, women

<https://policies.yahoo.com/us/en/yahoo/privacy/index.htm>

24. Yahoo represented to Plaintiffs and the other class members that its PI databases were secure and that customers' PI would remain private. In particular, Yahoo represented that "protecting our systems and our users' information is paramount to ensuring Yahoo users enjoy a secure user experience and maintaining our users' trust." *<https://policies.yahoo.com/us/en/yahoo/privacy/topics/security/index.htm>*. Yahoo further assured users that "We have physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you." *<https://policies.yahoo.com/us.en/yahoo/privacy/index.htm>*



25. But, on or about September 22, 2016, Yahoo informed its users that they were victims of a massive data breach, dating back to 2014. Yahoo said in a statement that "the account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt) and, in some cases, encrypted or unencrypted security questions and answers."

26. Yahoo said it believed a "state-sponsored actor" was behind the data breach, meaning an individual acting on behalf of a government. Yahoo stated that the breach occurred in late 2014, and it estimated that data from at least 500 million user accounts was stolen in what is believed to be the largest cybersecurity breach ever.

27. This is not the first such breach for Yahoo. In 2012, Yahoo admitted that more than 450,000 user accounts were compromised. This should have served as a "wake up call" to Yahoo that its protections for users' personal information were inadequate, but Yahoo did not fix the known holes in its security.

28. In its September 22, 2016 statement, Yahoo claims it did not uncover the current breach until two years after it happened. But Yahoo has been less than forthcoming, as illuminated in a September 23, 2016, Financial Times report that stated that "Yahoo CEO Marissa Mayer has known that Yahoo was investigating a serious data breach since July, but withheld the information from investors, regulators and acquirer Verizon until this week…" *http://www.cnbc.com/2016/09/23/yahoo-ceo-mayer-knew-about-data-breach-in-july-report.html*.

29. Indeed, an article posted on the technology website Motherboard on August 1, 2016, stated "A notorious cybercriminal is advertising 200 million of alleged Yahoo user credentials on the dark web, and the company has said it is 'aware' of the hacker's claims, but has not confirmed nor denied the legitimacy of the data." *http://motherboard.vice.com/read/yahoo-supposed-data-breach-200-million-credentials-dark-web.*

30. Yahoo had reason to keep any breach under wraps. It struggled for years to compete with more successful technology giants and is now in the midst of a sale of its core business to Verizon for $4.8 billion.

31. Yahoo's lack of timeliness upset several United States senators. On September 27, 2016, after Yahoo's belated disclosure of the breach, six senators sent Yahoo CEO Marissa Mayer a letter outlining several concerns. Particularly troubling to the senators was Yahoo's failure to notify its users of the breach sooner:

United States Senate
WASHINGTON, DC 20510

September 27, 2016

Ms. Marissa Mayer
Chief Executive Officer
Yahoo Inc.
701 First Avenue
Sunnyvale, CA 94089

Dear Ms. Mayer:

We write following your company's troubling announcement that account information for more than 500 million Yahoo users was stolen by hackers, compromising users' personal information across the Yahoo platform and on its sister sites, including Yahoo Mail, Flickr, Yahoo Finance, and Yahoo Fantasy Sports. The stolen data included usernames, passwords, email addresses, telephone numbers, dates of birth, and security questions and answers. This is highly sensitive, personal information that hackers can use not only to access Yahoo customer accounts, but also potentially to gain access to any other account or service that users access with similar login or personal information, including bank information and social media profiles.

> We are even more disturbed that user information was first compromised in 2014, yet the company only announced the breach last week. That means millions of Americans' data may have been compromised for two years. This is unacceptable. This breach is the latest in a series of data breaches that have impacted the privacy of millions of American consumers in recent years, but it is by far the largest. Consumers put their trust in companies when they share personal and sensitive information with them, and they expect all possible steps be taken to protect that information.

32. By failing to disclose the breach in a timely manner, despite knowing about it, Yahoo misled consumers into continuing to sign up for Yahoo services and products, thus providing Yahoo a continuing income stream. This, in turn allowed Yahoo to prop up its stock price and maximize profits to Yahoo shareholders (including Yahoo officers) in the sale to Verizon.

33. As reported on CNBC, "Due to the scale of the Yahoo breach, and because users often recycle passwords and security answers across multiple services, cyber security experts warned the impact of the hack could reverberate throughout the internet." *http://www.cnbc.com/2016/09/23/after-yahoo-data-breach-some-angry-users-close-accounts.html*.

34. In the wake of this breach, Senator Mark Warner, a co-founder of Nextel, has called on the Securities and Exchange Commission to investigate whether Yahoo properly notified the public of the massive breach.

35. The type of information compromised in this data breach is highly valuable to perpetrators of identity theft. Names, email addresses, telephone numbers, dates of birth, passwords and security question answers, as well as, obviously, credit and debit card information, can all be used to gain access to a variety of existing accounts and websites. Indeed, named plaintiffs and unnamed class members have suffered a variety of consequences from the breach, including forged credit applications, fake IRS tax returns being filed under the user's name, fraudulent charges, email hacks, and numerous other identity theft-related damages.

36. In addition to compromising existing accounts, the class members' PI can be used by identity thieves to open new financial accounts, incur charges in the name

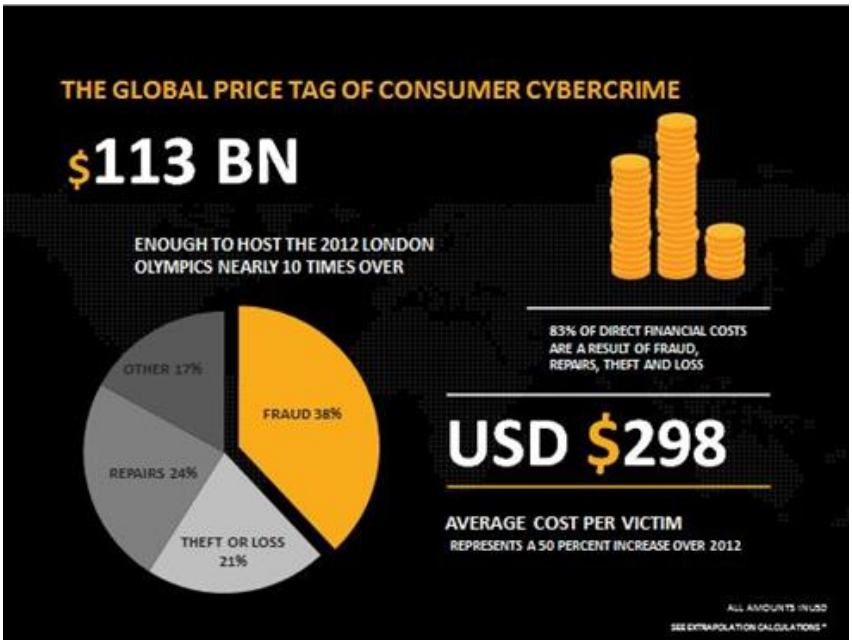
of class members, take out loans, clone credit and debit cards, and other unauthorized activities.

37. Identity thieves can also use the PI to harm the class members through embarrassment, blackmail or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits. A Presidential Report on identity theft from 2008 states that:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, at p.11 (April 2007), available at <*http://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf*>.

38. To put it into context, the 2013 Norton Report, based on one of the largest consumer cybercrime studies ever conducted, estimated that the global price tag of cybercrime is around $113 billion, with the average cost per victim being $298 dollars:



39. These problems are exacerbated by the fact that many identity thieves will wait years before attempting to use the personal information they have obtained. A Government Accountability Office ("GAO") study found that "stolen data may be held for up to a year or more before being used to commit identity theft." In order to protect themselves, class members will need to remain vigilant against unauthorized data use for years and decades to come. GAO, Report to Congressional Requesters, at p. 33 (June 2007), available at <www.gao.gov/new.items/d07737.pdf>

40. Plaintiffs and class members are at risk for identity theft in its myriad forms, potentially for the remainder of their lives.

41. Yahoo users whose PI has been unlawfully accessed or stolen can—and should—sign up for credit protection services immediately. Such services cost money, however. For example, according to the California Department of Justice, the three main credit bureaus charge $10 each to "freeze" credit files. (*https://oag.ca.gov/idthemf/facts/freeze-your-credit*). Yahoo has yet to offer to reimburse such costs for the millions of users affected by the breach.

Class Action Allegations

42. Plaintiffs bring this lawsuit on behalf of themselves and as a class action on behalf of a proposed national class, defined as:

> All persons in the United States who were or are Yahoo account holders and whose personal or financial information was accessed, compromised, or stolen from Yahoo in the data breach first publicly announced by Yahoo on or around September 22, 2016 (which breach, according to Yahoo, occurred in or around late 2014).

43. Plaintiffs also bring this lawsuit on behalf of themselves and as a subclass, defined as:

> All persons in the State of California who were or are Yahoo account holders and whose personal or financial information was accessed, compromised, or stolen from Yahoo in the data breach first publicly announced by Yahoo on or around September 22, 2016 (which breach, according to Yahoo, occurred in or around late 2014).

44. Collectively, the national class and California subclass will be referred to as "the Class."

45. Excluded from the Class are Defendants and any entities in which Defendant or their subsidiaries or affiliates have a controlling interest; Defendant's officers, agents, and employees; attorneys for Plaintiffs and the Class; the judicial officer to whom this action is assigned and any member of the Court's staff and immediate families; as well as claims for personal injury, wrongful death, and emotional distress.

46. **Numerosity:** The members of the Class are so numerous that joinder of all members would be impracticable. Plaintiffs reasonably believe that class members number millions of people. As such, class members are so numerous that joinder of all members is impractical. The names and addresses of class members are identifiable through documents maintained by Yahoo.

47. **Commonality and Predominance:** This action involves common questions of law or fact, which predominate over any questions affecting individual class members, including:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant owed a legal duty to Plaintiffs and the other class members to exercise due care in collecting, storing, and safeguarding their Personal Information;

c. Whether Defendant negligently or recklessly breached legal duties owed to Plaintiffs and the other class members to exercise due care in collecting, storing, and safeguarding their Personal Information and financial information;

d. Whether Defendant's conduct violated Cal. Civ. Code § 1750 *et seq.*

e. Whether Defendant's conduct violated Cal. Bus. & Prof. Code § 17200 *et seq.*;

f. Whether Defendant's conduct violated Cal. Civ. Code § 1798.80 *et seq.*;

g. Whether Plaintiffs and the other class members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

h. Whether Plaintiffs and the other class members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

48. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of the other class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

49. **Typicality:** Plaintiffs' claims are typical of the claims of the other class members because, among other things, Plaintiffs and the other class members were

injured through the substantially uniform misconduct by Yahoo. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other class members, and there are no defenses that are unique to Plaintiffs.

50. **Adequacy of Representation:** Plaintiffs are adequate representatives of the class because their interests do not conflict with the interests of the other class members they seek to represent; they have retained counsel competent and experienced in complex class action litigation and Plaintiffs will prosecute this action vigorously. The class' interests will be fairly and adequately protected by Plaintiffs and their counsel.

51. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the other class members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for class members to individually seek redress for Defendant's wrongful conduct. Even if class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments, and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

52. **Application of California law** – Because Yahoo is headquartered in California and all of its key decisions and operations emanate from California, California law can and should apply to claims relating to the data breach, even those made by persons who reside outside of California. Additionally, Yahoo's Terms of Service, to the extent applicable, contain a choice of law provision specifying Yahoo's

understanding that it may be held accountable under California law regardless of the location of the user.

FIRST CLAIM FOR RELIEF

Violation of California's Unfair Competition Law ("UCL") (Cal. Bus. & Prof. Code § 17200 *et seq*.)

53. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in each and every paragraph above, as though fully stated herein.

54. Defendant Yahoo engaged in unfair, unlawful, and fraudulent business practices in violation of the UCL.

55. By reason of the conduct alleged herein, Yahoo engaged in unlawful, unfair, and deceptive practices within the meaning of the UCL. The conduct alleged herein is a "business practice" within the meaning of the UCL.

56. Defendant stored Plaintiffs' and the other class members' PI in their electronic and consumer information databases. Yahoo represented to Plaintiffs and the other class members that its PI databases were secure and that customers' PI would remain private. Yahoo engaged in deceptive acts and business practices by providing in its website that "protecting our systems and our users' information is paramount to ensuring Yahoo users enjoy a secure user experience and maintaining our users' trust" and by representing that it has "physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you." (*https://policies.yahoo.com/us/en/yahoo/privacy/topics/security/index.htm*); (https://policies .yahoo.com/us/en/yahoo/privacy/index.htm).

57. Yahoo knew or should have known that it did not employ reasonable measures that would have kept Plaintiffs' and the other class members' PI and financial information secure and prevented the loss or misuse of Plaintiffs' and the other class members' PI and financial information.

58. Yahoo's representations that it would secure and protect Plaintiffs' and the other class members' PI and financial information in its possession were facts that

reasonable persons could be expected to rely upon when deciding whether to use Yahoo's services.

59. Defendant violated the UCL by misrepresenting the safety of their many systems and services, specifically the security thereof, and their ability to safely store Plaintiffs' and Class Members' PI. Yahoo also violated the UCL by failing to immediately notify Plaintiffs and the other Class members of the data breach. If Plaintiffs and the other Class members had been notified in an appropriate fashion, they could have taken precautions to safeguard their PI.

60. Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, Cal. Civ. Code § 1750 *et seq.*, Cal. Civ. Code § 1798.80 *et seq.*, and 18 U.S.C. § 2702, and also Cal. Bus. & Prof. Code § 22576 (as a result of Yahoo failing to comply with its own posted privacy policy).

61. Plaintiffs and the other Class members suffered injury in fact and lost money or property as the result of Defendant's failure to secure Plaintiffs' and the other Class members' PI contained in Defendant's servers or databases. In particular, Plaintiffs and class members have suffered from forged credit applications and tax returns; improper or fraudulent charges to their credit/debit card accounts; hacked emails; and other similar harm, all as a result of the data breach.

62. As a result of Yahoo's violations of the UCL, Plaintiffs and the other class members are entitled to restitution and injunctive relief.

SECOND CLAIM FOR RELIEF

Violation of California's Consumer Legal Remedies Act ("CLRA")

(Cal. Civ. Code § 1750 *et seq.*)

63. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in each and every paragraph above, as though fully stated herein.

64. The CLRA was enacted to protect consumers against unfair and deceptive business practices. It extends to transactions that are intended to result, or

which have resulted, in the sale of goods or services to consumers. Yahoo's acts, omissions, representations and practices as described herein fall within the CLRA.

65. Plaintiffs and the other class members are consumers within the meaning of Cal. Civ. Code §1761(d).

66. Yahoo's acts, omissions, misrepresentations, and practices were and are likely to deceive consumers. By misrepresenting the safety and security of their electronic, health, and customer information databases, Yahoo violated the CLRA. Yahoo had exclusive knowledge of undisclosed material facts, namely, that their consumer databases were defective and/or unsecure, and withheld that knowledge from Plaintiffs and the other class members.

67. Yahoo's acts, omissions, misrepresentations, and practices alleged herein violated the following provisions of the CLRA, Civil Code § 1770, which provides, in relevant part, that:

> (a) The following unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services to any consumer are unlawful:
>
> > (5) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have . . .
> >
> > (7) Representing that goods or services are of a particular standard, quality, or grade . . . if they are of another.
> >
> > (14) Representing that a transaction confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law.
> >
> > (16) Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

68. Defendant stored Plaintiffs' and the other class members' PI in its electronic and consumer information databases. Defendant represented to Plaintiffs

and the other class members that their PI databases were secure and that customers' PI would remain private. Yahoo engaged in deceptive acts and business practices by providing in its website that "protecting our systems and our users' information is paramount to ensuring Yahoo users enjoy a secure user experience and maintaining our users' trust" and by representing that it has "physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you." (*https://policies.yahoo.com/us/en/yahoo/privacy/topics/security/index.htm*)

69. Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiffs' and the other class members' Personal Information or financial information secure and prevented the loss or misuse of that information.

70. Defendant's deceptive acts and business practices induced Plaintiffs and the other class members to use Yahoo's online services, and to provide their PI and financial information. But for these deceptive acts and business practices, Plaintiffs and the other class members would not have provided that information to Defendant.

71. Plaintiffs and the other class members were harmed as the result of Defendant's violations of the CLRA, because their PI and financial information were compromised, placing them at a greater risk of identity theft and their PI and financial information disclosed to third parties without their consent.

72. Plaintiffs and the other class members suffered injury in fact and lost money or property as the result of Defendant's failure to secure Plaintiffs' and the other class members' PI and financial information.

73. As the result of Defendant's violation of the CLRA, Plaintiffs and the other class members are, or will be, entitled to compensatory and exemplary damages, an order enjoining Defendant from continuing the unlawful practices described herein, a declaration that Defendant's conduct violated the CLRA, attorneys' fees, and the costs of litigation.

74. Pursuant to Civil Code § 1782, concurrent with the filing of the original Complaint in this action, Plaintiffs notified Defendant in writing by certified mail of

the alleged violations of section 1770 and demanded that the same be corrected. Concurrent with the filing of this First Amended Complaint, Plaintiffs will provide further notification to Defendant in writing by certified mail pursuant to Section 1782, and again demand that Defendant's Section 1770 violations be corrected. If Defendant fails to rectify or agree to rectify the problems associated with the action detailed above within 30 days of the date of written notice pursuant to Civil Code § 1782, Plaintiffs will amend this Complaint to add claims for actual, punitive and statutory damages, as appropriate in accordance with Civil Code § 1782(a) & (d).

THIRD CLAIM FOR RELIEF

Violation of Cal. Civ. Code § 1798.80 *et seq*.

75. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in each and every paragraph above, as though fully stated herein.

76. Section 1798.82 of the California Civil Code provides, in pertinent part:

> (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
>
> (b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
>
> (c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) Any person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language.

(2) The security breach notification shall include, at a minimum, the following information:

(A) The name and contact information of the reporting person or business subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

* * * * * * *

(f) Any person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

> (g) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

77. The breach described previously in this Complaint constituted a "breach of the security system" of Yahoo.

78. As alleged above, Yahoo unreasonably delayed informing anyone about the breach of security of Plaintiffs' and other class members' confidential and non-public PI and financial information after Defendant knew the breach had occurred.

79. Yahoo failed to disclose to Plaintiffs and other class members, without unreasonable delay, and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, PI and financial information when they knew or reasonably believed such information had been compromised.

80. Yahoo's ongoing business interests, and in particular its impending sale to Verizon, gave Yahoo incentive to want to conceal the breach from the public to ensure continued revenue and a high stock price for the sale.

81. Upon information and belief, no law enforcement agency instructed Yahoo that notification to Plaintiffs or other class members would impede its investigation.

82. Pursuant to Section 1798.84 of the California Civil Code:

> (a) Any waiver of a provision of this title is contrary to public policy and is void and unenforceable.
>
> (b) Any customer injured by a violation of this title may institute a civil action to recover damages.

> (c) In addition, for a willful, intentional, or reckless violation of Section 1798.83, a customer may recover a civil penalty not to exceed three thousand dollars ($3,000) per violation; otherwise, the customer may recover a civil penalty of up to five hundred dollars ($500) per violation for a violation of Section 1798.83.
>
> * * * * * * *
>
> (e) Any business that violates, proposes to violate, or has violated this title may be enjoined.

83. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiffs and the other class members incurred economic damages relating to expenses for credit monitoring, loss of use and value of their debit and/or credit cards, and loss of rewards on their debit and/or credit cards.

84. Plaintiffs, on behalf of themselves and the class, seeks all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to: (a) damages suffered by Plaintiffs and the other class members as alleged above; (b) statutory penalties of up to $3,000 per violation for Defendant's willful, intentional, and/or reckless violations of Cal. Civ. Code § 1798.83 (or, at a minimum, up to $500 per violation); and (c) equitable relief.

85. Plaintiffs and the Class also seeks reasonable attorneys' fees and costs under Cal. Civ. Code §1798.84(g).

FOURTH CLAIM FOR RELIEF

Negligence

86. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in each and every paragraph above, as though fully stated herein.

87. Yahoo owed a duty to Plaintiffs and the other class members to exercise reasonable care in safeguarding and protecting their PI and financial information that was in its possession from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendant's security systems to ensure that Plaintiffs' and

the other class members' PI and financial information was adequately secured and protected. Defendant further had a duty to implement processes that would detect a breach of their security system in a timely manner.

88. Yahoo also had a duty to timely disclose to Plaintiffs and the other class members that their PI and financial information had been or was reasonably believed to have been compromised. Timely disclosure was appropriate so that, among other things, Plaintiffs and the other class members could take appropriate measures to cancel or change usernames, pin numbers, and passwords on compromised accounts, to begin monitoring their accounts for unauthorized access, to contact the credit bureaus to request freezes or place alerts, and take any and all other appropriate precautions.

89. Yahoo breached is duty to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other class members' PI and financial information by failing to adopt, implement, and maintain adequate security measures to safeguard that information; allowing unauthorized access to Plaintiffs' and the other class members' PI and financial information stored by Defendant; and failing to recognize in a timely manner the breach.

90. Yahoo breached its duty to timely disclose that Plaintiffs' and the other class members' PI and financial information had been, or was reasonably believed to have been, stolen or compromised.

91. Yahoo's failure to comply with industry regulations and the delay between the date of intrusion and the date Yahoo informed customers of the data breach further evidence Yahoo's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other class members' PI and financial information.

92. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and the other class members, their PI and financial information would not have been compromised, stolen, and viewed by unauthorized persons.

93. The injury and harm suffered by Plaintiffs and the other class members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other class members' PI and financial information. Defendant knew or should have known that their systems and technologies for processing and securing Plaintiffs' and the other Class members' PI and financial information had security vulnerabilities.

94. As a result of Defendant's negligence, Plaintiffs and the other class members incurred economic damages, including expenses for credit monitoring, fraudulent charges on credit card or bank accounts, forged IRS returns, loss of use and value of their debit and/or credit cards, and/or other identity theft-related damages.

FIFTH CLAIM FOR RELIEF

Violation of Stored Communications Act, 18 U.S.C. § 2702

95. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in each and every paragraph above, as though fully stated herein.

96. The Federal Stored Communications Act ("SCA") contains provisions that provide consumers with redress if a company mishandles their electronically stored information. The SCA was designed, in relevant part, "to protect individuals' privacy interests in personal and proprietary information." S. Rep. No. 99-541, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555 at 3557.

97. Section 2702(a)(1) of the SCA provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

98. The SCA defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." *Id.* at § 2510(15).

99. Through its equipment, Defendant provides an "electronic communication service to the public" within the meaning of the SCA because it

provides consumers at large with mechanisms that enable them to send or receive wire or electronic communications concerning their private financial information to transaction managers, card companies, or banks.

100. By failing to take commercially reasonable steps to safeguard sensitive private financial information, even after Defendant was aware that customers' PI and financial information had been compromised, Defendant knowingly divulged customers' private financial information that was communicated to financial institutions solely for customers' payment verification purposes, while in electronic storage in Defendant's payment system.

101. Section 2702(a)(2)(A) of the SCA provides that "a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service." 18 U.S.C. § 2702(a)(2)(A).

102. The SCA defines "remote computing service" as "the provision to the public of computer storage or processing services by means of an electronic communication system." 18 U.S.C. § 2711(2).

103. An "electronic communications systems" is defined by the SCA as "any wire, radio, electromagnetic, photo-optical or photo-electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(4).

104. Defendant provides remote computing services to the public by virtue of its computer processing services for consumer credit and debit card payments, which are used by customers and carried out by means of an electronic communications system, namely the use of wire, electromagnetic, photo-optical or photo-electric

facilities for the transmission of wire or electronic communications received from, and on behalf of, the customer concerning customer private financial information.

105. By failing to take commercially reasonable steps to safeguard sensitive private financial information, even after Defendant was aware that customers' PI and financial information had been compromised, Defendant has knowingly divulged customers' private financial information that was carried and maintained on Defendant's remote computing service solely for the customer's payment verification purposes.

106. As a result of Defendant's conduct described herein and their violations of Section 2702(a)(1) and (2)(A), Plaintiffs and the class members have suffered injuries, including lost money and the costs associated with the need for vigilant credit monitoring to protect against additional identity theft. Plaintiffs, on their own behalf and on behalf of the putative class, seeks an order awarding themselves and the class the maximum statutory damages available under 18 U.S.C. § 2707 in addition to the cost for 3 years of credit monitoring services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other Class members, respectfully requests that this Court enter an Order:

(a) Certifying the Class and the Subclass, appointing Plaintiffs as Class Representatives, and appointing their undersigned counsel as Class Counsel;

(b) Finding that Defendant's conduct was negligent, deceptive, unfair, and unlawful as alleged herein;

(c) Enjoining Defendant from engaging in the negligent, deceptive, unfair, and unlawful business practices alleged herein;

(d) Awarding Plaintiffs and the other class members actual, compensatory, and consequential damages;

(e) Awarding Plaintiffs and the other class members statutory damages and penalties;

(f) Awarding Plaintiffs and the other class members restitution and disgorgement;

(g) Requiring Defendant to provide appropriate credit monitoring services to Plaintiffs and the other class members;

(h) Awarding Plaintiffs and the other class members pre-judgment and post-judgment interest;

(i) Awarding Plaintiffs and the other class members reasonable attorneys' fees and costs, including expert witness fees, and;

(j) Granting such other relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this First Amended Class Action Complaint so triable.

Dated: September 30, 2016

CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP

ZAVERI TABB, APC

s/ Wendy M. Behan
wbehan@cglaw.com
Attorneys for Plaintiffs